5. *Цапко Г. П.* Анализ рисков безопасности автоматизированных систем управления технологическими процессами // Интернет-журнал «Науковедение». 2016. № 5. С 1–9.

УДК 004.056.53

И. П. Соколов
Научный руководитель: канд. тех. наук, доцент В. В. Бакланов
Уральский федеральный университет, Екатеринбург

О БЕЗОПАСНОСТИ ПРОГРАММ С ОТКРЫТЫМ КОДОМ

Аннотация: обсуждаются проблемы информационной безопасности LINUX-программ с открытым кодом.

Ключевые слова: программное обеспечение с открытым кодом; операционная система LINUX; сетевой протокол.

Сегодня широкое распространение получили программные продукты и системы с открытым исходным кодом. Это объясняется тем, что они бесплатные и, по мнению многих, безопасные, поскольку используют открытый исходный код, который может проверить каждый желающий. С далеких времен яркими представителями операционных систем с открытым исходным кодом являются UNIX подобные системы, которые развивались энтузиастами, и порой о безопасности никто и не думал.

С появлением Linux ничего не изменилось, Linux целиком соблюдает концепции, заложенные в UNIX. Ядро Linux полностью свободно распространяемое, как и утилиты, входящие в ее комплект. Многие считают Linux неуязвимой системой. Однако Linux-системы, как выше упоминалось, разрабатываются энтузиастами, и они значительно проигрывают системам, которые разрабатываются специализированными организациями. Например, над разработкой ОС семейства Windows работают тысячи высококвалифицированных разработчиков, но даже в этом семействе операционных систем периодически находят уязвимости. Кроме того, в Linux принято латать ядро, а старинные утилиты, которые перекочевывают из дистрибутива в дистрибутив, никто не анализирует и не переписывает. Например, последнее изменение в пакете kbd датируется 2002 годом [1].

Новые системы, создаваемые на базе Linux, просто копируют базовый дистрибутив и дополняют его, не проверяя содержимое этих дистрибутивов и не исследуя старые утилиты, содержащиеся в этих дистрибутивах, в итоге полу-

чая псевдозащищенные системы, в которых обновляется ядро и забываются старые утилиты, которыми уже и не пользуются.

Сегодня множество пакетов, а это достаточное количество различных утилит, не используются пользователем. Пример таких утилит — это утилиты настройки работы в виртуальных терминалах, утилиты настройки работы клавиатуры в виртуальных терминалах. Кто их использует? Никто. Даже в крупных IT-компаниях, которые разрабатывают программное обеспечение, программисты используют графический режим работы. Более того, 90 % работ по локальной настройке операционных систем пользователей системные администраторы выполняют в графическом режиме. Настройка серверов осуществляется с помощью ssh консоли, которая на конечном устройстве задействует псевдотерминальное устройство pts и не поддается настройке, для которой были созданы вышеупомянутые пакеты утилит [2].

В итоге мы получаем огромное количество ненужных утилит, которые могут быть использованы злоумышленником в коростных целях. Например, нигде не документировано, что утилита showkey может использоваться как кей логер. Однако применение в качестве кей логера утилиты showkey позволяет злоумышленнику не только оставаться незамеченным для различного рода систем безопасности, но и благополучно перехватывать все события клавиатуры, в том числе если доступ к удаленному серверу осуществляется по ssh.

В старинных утилитах используются вызовы ядра ioctl, про которые разработчики ядра давно забыли. Например, ничто не мешает пользователю, используя утилиту vt, переместится в терминал администратора и при этом остаться незаметным, что также не является безопасным, поскольку подобные вызовы ioctl не отслеживаются логами системы.

Кроме старинных утилиты, в Linux-системах остались различные службы, которые неизвестно для чего и кем были созданы. Их код, как правило, не документирован.

Также опасным является то, что каждый дистрибутив Linux, «таскает» за собой старинные сетевые протоколы, которыми никто в наше время не пользуется. Что позволяет сделать вывод о том, что пакетная поставка дистрибутивов не является корректной и безопасной и зачастую несет в своем составе объекты, которых уже давно не должно быть.

В качестве исследуемых дистрибутивов были выбраны те, которые базируются на дистрибутиве Debian, это Ubuntu, Slackware, Linux Mint. В качестве исследуемого пакета был выбран пакет kbd, содержащий в себе утилиты, которые могут быть интересны злоумышленнику, а также различные системные вызовы и структуры по настройки виртуального терминала. В результате исследования, были получены утилиты, которые могут быть использованы внутренним и внешним нарушителем в корыстных целях.

Таким образом, можно сделать вывод, что на сегодняшний день самой большой угрозой является терминальный режим, старинные сетевые протоколы, службы, которые никто не использует, но они «кочуют» из дистрибутива в дистрибутив. Разработчикам дистрибутивов стоит провести анализ и убрать лишние пакеты из своих дистрибутивов.

Список литературы

1. Сайт разработчиков ОС Debian. https://www.debian.org.
2. *Корбет Д., Рубини А.* Драйверы устройств Linux // США O'Reilly Media Inc, 2005.

УДК 004.056.2

И. А. Корелин, Т. М. Мкртчян
Научный руководитель: д-р тех. наук, профессор С. В. Поршнев
Уральский федеральный университет, Екатеринбург

ЖИЗНЕОБЕСПЕЧЕНИЕ ЦЕНТРА ОБРАБОТКИ ДАННЫХ: ЗАЩИТА И РИСКИ. ФИЗИЧЕСКАЯ ЗАЩИЩЕННОСТЬ

Аннотация. В статье анализируется несколько вариантов физической защищенности центра обработки данных (ЦОД). Результаты исследования получены на основе системного и процессного подходов. Для оценки результативности исследования автор изучил количественные и качественные методы анализа физической защищенности центра обработки данных. На основе полученных результатов разработаны рекомендации по улучшению качества обслуживания информации, хранящийся на любом электронном носителе. Основная цель физической защищенности — это надежная сохранность любой информации, полученной от клиентов. Также в статье рассматриваются наиболее эффективные и безопасные методы хранения информации. Это позволяет выявлять потенциальных клиентов с помощью ЦОД, обеспечивая необходимые условия для удовлетворения их потребности: сохранности информации.

Ключевые слова: защищенность; процессный подход; услуги; ЦОД; охрана; видеонаблюдение; система; безопасность.

Процесс обмена данными практически полностью перешел в сферу Интернета. Информация стала ценным продуктом на мировом рынке: за сведения о клиентах, конкурентах, своих сотрудниках готовы платить многие компании и частные лица, что увеличивает риск похищения таких данных. Все чаще ЦОД